The Office for Domestic Preparedness

Prevention Guidelines for Homeland Security

June 2003

Introduction

The preeminence of prevention as a component of Homeland Security is made clear in the opening statements of the Executive Summary, **The National Strategy for Homeland Security**:

> The strategic objectives of homeland security in order of priority are to:
>
> - Prevent terrorist attacks within the United States;
> - Reduce America's vulnerability to terrorism, and;
> - Minimize the damage and recover from attacks that may occur.[1]

Within the text of that document, the meaning is unambiguous. Even the definition of Homeland Security makes prevention an imperative: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover form attacks that do occur."[2]

Prevention is a broad term that is often contextually defined. In the context of terrorism employing Weapons of Mass Destruction (WMD), the **National Strategy for Homeland Security** includes the following elements under prevention:

- "deter all potential terrorists from attacking America through our uncompromising commitment to defeating terrorism wherever it appears."
- "detect terrorists before they strike."
- "prevent them and their instruments of terror from entering our country."
- "take decisive action to eliminate the threat they pose."[3]

In September, 2002, the Office for Domestic Preparedness (ODP) began a "task analysis" process to identify, in the opinion of multi-disciplinary, multi-wave Subject Matter Experts, some of the key elements of "Prevention" within the framework of WMD Terrorism and Homeland Security. The process began with open-ended responses to the following:

> At this stage, we are simply soliciting the insight and comments of the Subject Matter Experts (SMEs) regarding the objectives which are most appropriate to prevention of WMD attacks and threats of terrorism, of all varieties (Nuclear, Biological, Chemical, Incendiary, Explosive, Cyber/Technological).

The comments were lengthy and, once collated and organized, coalesced logically into categories. The next step in the process involved SMEs revising, elaborating upon, and rating the importance of the tasks identified in the first solicitation. The tasks were then screened, collapsed where possible, and the most critical tasks listed. These tasks do not represent a comprehensive list because such a list would be impossible to develop in this time of emerging threats and innovative tactics. Rather, these tasks reflect a base of key actions or activities representing a **"framework for prevention"** that each jurisdiction should consider in adapting to the exigencies of terrorism.

---

[1] Office of Homeland Security. (2002). **National Strategy for Homeland Security**. Washington, DC: Government Printing Office. P.vii.
[2] Ibid. P. 2.
[3] Ibid..

Application of the Guidelines

These Guidelines represent, at this stage of development, a set of general activities, objectives, and elements that organizations as well as well as those in command positions within the organizations should consider in the development of prevention plans. The Guidelines are divided into the functional categories of Collaboration, Information Sharing, Threat Recognition, Risk Management, and Intervention. Prevention, if it is to be effective, begins before a response is necessary. The tasks and activities in this booklet, however, make it clear that preventing further harm is a necessary aspect of prevention and one that makes prevention and response seamless.

Collaboration is critical if agencies, organizations and jurisdictions are to develop a framework for prevention. Describing tasks as Law Enforcement, Fire, Emergency Management Agency, Public Health, etc. seems to suggest maintaining the "stovepipes" that are often impediments to collaboration. We propose that the tasks and activities suggested in the Guidelines be considered by ***Jurisdictions***, and the responsibilities for action and implementation be determined collaborative within those jurisdictions, based on resources, agencies, and personnel.

Establishing the "Jurisdiction" as the locus of activity, control, and responsibility, we recommend that policy makers and stakeholders collaboratively address each of the tasks listed below, defining each in the context of the organizations at the local, regional, state, and federal levels, with which they have relationships, and establish a "framework for prevention" unique to the sources, capabilities, threats, vulnerabilities, and risks, as well as the resources available to the jurisdiction.

If the activities delineated below are considered, it is likely a "cultural shift" will occur among the public safety agencies, organizations and personnel. This "cultural shift" is more a product of the process than an intended consequence. The Subject Matter Experts in a recent panel stated:

As a consequence of the collaboration, information sharing, and coordinated activities inherent in adopting and executing a Risk Management Model or some other analytical risk and vulnerability model, it is expected that there will be a "Cultural Shift" in the public safety community. The "Cultural Shift" will occur through a process including:

- –Identify a prime mover (an organization, person, or event)
- –Identify public and private Stakeholders
- –Establish Meeting(s) of the Stakeholders to:
  - •Articulate the Mission, Goals, Objectives in Preventing terrorism
  - •Plan Joint/Integrated Training & Awareness Training
  - •Plan Joint Exercises
  - •Adopt a Risk Management Decision Model
  - •Develop MOUs and Policies to enable cooperation
  - •Centralize an Information Management System and Fusion Center
  - •Define agency or individual responsibility for all of the Prevention tasks and activities described in the Guidelines, appropriate to the jurisdiction.

The shared motivation (fiscal support, public safety, proactive steps to deter and prevent attacks) should produce shared values in existing organizations and personnel, and the values should become "organic" and perpetuated through pre-service training as well as in-service training and exercises.

We include the information on this "Cultural Shift" because it represents a significant element of the overarching process jurisdictions should consider in implementing a "framework for prevention" and applying these Guidelines.

The Glossary accompanying the Guidelines, provides specific definitions and descriptions, as well as reference sources for further guidance. While there are other definitions that could have been used, these definitions represent the reference points for the Subject Matter Experts considering the issues associated with Prevention and the development of the Guidelines. The Glossary was not intended to be comprehensive in addressing all terms and terminology related to WMD terrorism, but to articulate and define the terms associated with this document.

It is noted that this document, and the accompanying Glossary, are still in Draft form. SMEs continue to refine and append the materials with the objective of improving the comprehensiveness and the specificity. The Guidelines are likely to always be "in progress" and subject to revision, but they are being released so that agencies, organizations, and jurisdictions can begin to benefit from the work of ODP and Subject Matter Experts over the past months.

Jurisdictions seeking to improve "Collaborations" between and among public and private sector agencies to prevent WMD terrorism should:

1. **Establish the recognition that there is a need for prevention activities and actions and that prevention is critical to a jurisdiction's preparation for terrorism.**
   - Provide the political leadership with sufficient "awareness" and "process" training so that they will develop an appreciation for the importance of prevention;
   - Acquaint policy makers with the role governmental administrators play in preventing attacks, and reducing vulnerability;
   - Ensure that plans for WMD incorporate and begin with prevention activities;
   - Establish policies, budgets, and plans that reflect prevention priority;
   - Reinforce the priority of prevention through exercises and scenarios.

2. **Establish a system, center, or task force to serve as a "clearing house" for all potentially relevant domestically generated terrorism data and information, ensuring interpretation and assessment of the data and information.**

- Follow provisions of 28 Code of Federal Regulations (CFR) pertaining to Criminal Intelligence Systems operating policies (Chapter 1, Part 23 in particular);
- Establish an all source intelligence fusion center;
- Prioritize the intelligence fusion center services to accommodate the task force as one of its principal accounts;
- Conduct an information needs analysis as a component of the intelligence center or system;
- Ensure that intelligence requirements are formulated in a clear and concise manner;
- Ensure that the information gathering and sharing system includes all "owners" of key assets/critical infrastructure;
- Establish a workable and reasonable “tear-line” approach for the sharing of information with other agencies, jurisdictions, and the private sector;
- Ensure appropriate representation in the task force and in the Intelligence Center, including public and private representatives;
- Establish the information system using plans and processes that reasonably assure that all terrorist-related activity is reported to the system, fusion center or task force;
- Identify “intelligence requirements” with sufficient specificity to alert observers to watch for certain things, and train them to pass the information along to a central point;
- Establish coordination points with related agencies to share information, strategies, and tactics;
- Establish a clear path of information from observers (police, others) to the fusion center;
- Conduct education/training periodically to test observation of suspicious events and behaviors.

3. **Prepare MOUs and formal coordination agreements between appropriate agencies (public and private) describing mechanisms to exchange information regarding vulnerabilities and risks, coordination of responses, and processes to facilitate information sharing and multi-jurisdictional preemption of terrorist acts or events.**
   - Identify in the planning process and agreements the appropriate agencies, public and private, with a need to participate (that is, supply information and/or receive information and intelligence) in collaborative information sharing;
   - Identify in the agreements the types and parameters of information exchanged, including standard methods of defining data, information, vulnerabilities, and risks;
   - Establish formal agreements or MOUs that identify the agencies, the points of contact, and the parameters of exchanges of information;

- Ensure that the process of exchanging information accomplishes the collaboration among agencies and organizations;
- Include in the exchange of information, on a need to know basis, blueprints, schematics, and other information on infrastructure.

4. **Use Community-policing initiatives, strategies, and tactics as a basis to identify suspicious activities related to terrorism.**
   - Train Law Enforcement in the jurisdiction to utilize community policing or other similar collaborative policing approaches, encouraging prevention, proactive policing, and close working relationships between the police and the community;
   - Train police officers to accomplish the mission, goals, and objectives of the community policing philosophy while engaging in prevention of terrorism and terrorist threats;
   - Provide examples, training, and materials (Public Service Announcements, videos, fliers, other media materials) to use Community policing contacts to make members of the community aware of those actions, behaviors, and events that constitute "suspicious" activity that may have value in recognizing terrorism;
   - Ensure that members of the community are aware of the means of and processes for relaying observed data to police officers and police organizations, just as they are or should be aware of methods to relay information to Community Policing officers;
   - Organize community meetings to emphasize prevention strategies, vigilance, and public awareness;
   - Train police officers to understand the legally appropriate response to data relayed by members of the community;
   - Train, prepare, and test police officers on the most appropriate and expedient methods for relaying the data to the intelligence center, fusion center, or task force for assessment, and analysis.

5. **Explicitly develop "social capital" through collaboration between the private sector, law enforcement and other partners so that data, information, assistance, and "best practices" may be shared and collaborative processes developed.**
   - Examine all plans and processes to ensure that they reflect clear linkages between public and private sectors and stakeholders;
   - Examine planning documents to ensure that fluid coordination is represented in the MOUs, task force organization, and other formal agreements;
   - Reserve task force seats for key private sector representatives;
   - Ensure that the planning documents and processes establish facility sharing and the sharing of resources as well as information;
   - Structure the information sharing, with appropriate legal limitations, so that private sector receives accurate, timely, and critical information, on a need to know basis;

- Establish a relationship of trust, leading to social capital, with the private sector as a partner in the information sharing relationships;
- Include in formal or informal relationships, private sector organizations that are representative groups such as the Chamber of Commerce;
- Establish multi-disciplinary cooperation, including the private sector, in target hardening activities, to include threat analysis, and risk management, matched with protocol and treatment;
- Employ practical exercises and assessment centers to reinforce the "social capital;"
- Use after action reports to identify ways to strengthen and perpetuate collaboration;
- Construct conceptual, structural, and strategic exercises and scenarios reinforce collaboration.

6. **Coordinate Federal, state, and local information, plans and actions for assessments, prevention procedures, infrastructure protection, and funding priorities to address prevention.**
   - Establish all-hazards councils with special conditions identifying dimensions including prevention for funding decisions with demonstrated cooperation and demonstrated activities associated with prevention;
   - Overtly develop an "inclusion strategy" as a measurable doctrine to influence the environment of stakeholder agencies;
   - Include prevention in a planning process similar to IMS/ICS but in a continuing process not simply during an "incident" or event;
   - Coordinate multi-disciplinary training and exercises for prevention, going beyond existing training and exercises for response;
   - Conduct training and exercises with sufficient frequency to ensure coordination;
   - Ascertain that every training curriculum includes an appropriate incident management system, such as the ICS model, to encourage understanding of roles and to facilitate coordination and cooperation horizontally and vertically;
   - Establish awareness training for all agencies and the public that includes protection measures and stresses collaboration;
   - Ensure coordination of training among all constituent jurisdictions so that consistent and coordinated models and approaches to risk identification and protection are used;
   - Participate in exercises to test collaboration and awareness or vulnerabilities and coordination of prevention approaches based on a risk management model;
   - Link coordination, training, and exercises on prevention to funding priorities.

7. **Establish a regional prevention information command center and coordinate the information in and information out regarding infrastructure.**
   - Establish MOUs and plans to coalesce cooperation and collaboration with all appropriate agencies creating a Joint Information Center for prevention;
   - Link fusion center activities to other-than-public safety organizations – transportation, public health, health services, and all other appropriate organizations;
   - Establish formal liaison with second and third responder agencies and organizations, as well as support organizations, to emphasize those agencies' roles in prevention;
   - Integrate regional prevention information centers with task forces, using a model consistent with the IMS/ICS model;
   - Establish "design, fabrication and construction monitoring" programs to provide consultation and advise regarding anti-terrorism measures.

8. **Exercise Prevention and Collaboration measures.**
   - Include prevention elements in every exercise, even those testing response, so that officials can see that, had those elements been recognized and acted upon, the event would have been altered or prevented;
   - In exercises, embed prevention cues that are or should be visible to agencies other than law enforcement, necessitating collaboration for the cues to be recognized and acted upon;
   - Make collaboration essential to the success of every exercise;
   - Adopt the proposition that "failures" in prevention exercises are "successes" in identifying gaps and areas for collaborative improvement, ultimately making the communities safer and more secure;
   - Conduct "red team" exercises to test collaboration dimension of prevention;
   - Coordinate multi-disciplinary training and exercises for prevention, going beyond existing training and exercises for response;
   - Conduct training and exercises with sufficient frequency to ensure coordination;
   - Examine all training curriculum to ensure that an appropriate incident management system, such as the IMS/ICS model is used, to encourage understandings of roles and facilitate coordination and cooperation horizontally and vertically;
   - Conduct awareness training for all agencies and the public, including prevention and protection measures and stressing collaboration;
   - Ensure coordination of training among all constituent jurisdictions so that consistent and coordinated models and approaches to risk identification, risk management, and protection are used;

- Participate in exercises to test collaboration and awareness of vulnerabilities and coordination of prevention approaches based on a risk management model;
- Link coordination, training, and exercises on prevention to funding priorities;
- Make funding conditional on degree of collaboration and exercise evaluations.

Jurisdictions seeking to develop "Information Sharing" linkages to prevent WMD terrorism should:

1. **Enhance analytic capabilities for linking information on potential threats.**
    - Train analyst to perform analysis, linkage, and fusion of data;
    - Identify the data categories most relevant to the threats defined;
    - Identify the data sources from whom or from which the data can be received, extracted, or collected;
    - Clearly define data gathering, analysis, and dissemination formats;
    - Identify the technology and techniques most appropriate to the analysis;
    - Disseminate information and intelligence on a need-to-know basis, defined *pre hoc* by a task force or other representative group;
    - Integrate public order issues, crime analysis, antiterrorism, and counterterrorism concerns with street level data and information.

2. **Establish a framework for sharing information/intelligence and prevention strategies, particularly between Law Enforcement and other agencies.**
    - Use joint terrorism task forces and the homeland security office in the state to facilitate information sharing;
    - Integrate Information Sharing into the "Intelligence Cycle;"
    - Establish data and information gathering, analysis, interpretation, and dissemination processes within Law Enforcement, oriented toward WMD terrorism;
    - Establish a "fusion center" for the accumulation of data, and clearly define the dissemination of data and information as well as intelligence.
    - To the extent possible, retain analytical dimensions in each organization, where data and information can best be understood and linked, after dissemination by fusion center;
    - Clearly articulate categories of data, information, and intelligence to be shared, as well as conduct and behaviors defined by the data.
    - Include in the information sharing framework private EMS and volunteer firefighters, with access based on need to know, and with appropriate limitations;
    - Establish a process for information sharing, across all tiers of government and the private sector, disseminated to the lowest organizational level possible to ensure that line personnel will receive appropriate information, on a need to know basis;
    - Review federal and state-level laws regulating gathering and acting upon information to ensure consistency with the framework for information gathering and sharing.

3. **Establish an information exchange network and directory for information sharing.**
    - Utilize existing systems, such as LEO, the Criminal Justice Information System, or other systems that are appropriately secure and capable of interfacing with other agencies;
    - Continue the process of developing next generation information systems that can better serve the agencies, organizations, and jurisdictions;
    - Include wireless and traditional Internet capabilities, for voice and data, as well as alternate infrastructure to promote rapid, secure, and accessible information sharing, such as Web and email;
    - Develop and maintain "call down" lists for each agency;
    - Design the Intelligence Cycle to ensure that all appropriate agencies and organizations (Public Health, EMA, EMS, Fire, selected Private Sector, etc.) at all tiers (local, regional, and state) receive restricted information on a need-to-know basis, defined in advance by the task force or central authority;
    - Examine the information sharing framework periodically to determine that all agencies are sharing appropriate information systematically;
    - Establish a system for disease surveillance, such as the Health Alert Network, insuring data interoperability in concert with Emergency Management Agency, and integrated into the information exchange network;
    - Consider ease of use and familiarity in defining the information network to ensure the information is accessible and usable;
    - Tie together the various analytic centers so that information and intelligence dissemination is comprehensive and consistent;
    - Review the participant agencies and organizations to be certain all appropriate representatives are linked to the information sharing system;
    - Evaluate the collection, assessment, storage, access, and dissemination of information periodically;
    - Establish basic standards by which the intelligence products are created and shared;
    - Establish protocols to insure that information is being shared with agencies and organizations overtly or potentially impacted by an identified threat;
    - Establish protocols to insure that information is being linked with the private sector, particularly that associated with critical infrastructure, on a need to know basis;
    - Disseminate valuable and *usable* information to agencies and organizations with threats or implicitly affected by the information.

4. **Ensure reliable capability to alert officials and emergency personnel of terrorism threats, with warnings initiated, received, and relayed to alert key decision makers and emergency personnel regardless of the threat or operational involvement, as well as a robust, redundant, timely system for sharing information with other agencies, organizations, and the public.**
    - Use a Risk Management Model or some appropriate analytical model to identify "hazards" and the appropriate information to be disseminated;
    - Test the process for implementing the model against a variety of threats and hazards;
    - Provide system redundancy to provide alternative communications using two-way communications, voice, and data;
    - Insure the system is compatible with internal and external communications systems of the parent organization.

5. **Establish a multi-disciplinary approach to public information for education and awareness and protective action information.**
    - Participate in public information campaigns to enhance awareness and public cooperation in information gathering;
    - Provide alert systems that can be implemented for hospitals, ERs, and private practice physicians;
    - Provide Public Health information to the public on vaccination risks and advantages.

6. **Develop an adaptive, organic architecture facilitating information sharing.**
    - Identify key stakeholders, contributors, and consumers of information;
    - Include stakeholders in planning process for information sharing;
    - Agree upon the location, structure, and funding for a centralized intelligence center or fusion center;
    - Select and train criminal intelligence analysts;
    - Secure access to all sources of data, information, and intelligence revising and refining sources constantly;
    - Adopt or develop a analytical model for assessing key assets, critical infrastructure, risk, vulnerability, and options for managing risk;
    - Test new sources and methods of information gathering and sharing to enhance the complex adaptive nature of the analysis process;
    - Establish clear methods for disseminating the intelligence products;
    - Provide for competent legal advice on the operation of the intelligence center or fusion center, the dissemination of information

and intelligence, and the actions taken based on the information and intelligence.

Jurisdictions considering "Risk Management"[4] approaches to reduce vulnerability of targets and prevent WMD terrorism should:

1. **Adopt or develop an appropriate analytic "risk management" model to assess risk or vulnerability and identify probable treatment methods to reduce risk.**

2. **Provide training and technical assistance to local governments in developing, adopting and implementing building codes, fire codes, and land-use ordinances, consistent with crime prevention methods.**

3. **Design the built environment to reduce vulnerability, being certain that Crime Prevention through Environmental Design (CPTED) principles and methods are available to agencies and organizations for the enhancement of "target hardening" of appropriate locations in the built environment.**

4. **Establish "anti-terrorism" Crime Prevention through Environmental Design (CPTED) "Target Hardening" activities.**
    - Assess threat, risk, and vulnerability;
    - Balance CPTED strategies against the threat, risk, and vulnerability;
    - Employ the appropriate CPTED measures, given the level of threat, risk, and vulnerability. Measures may include:
        - Install adequate security lighting;
        - Use planters and bollards as impediments or obstacles to prevent cars or trucks from driving into or parking too close to potential targets;
        - Use security cameras in key locations;
        - Increase police presence at sensitive locations;
        - Use random inspection of trucks/vans entering target-rich environments;
        - Establish protocol for searches of people and their possessions when entering large gatherings;
        - Adopt biometric technology, where applicable, to enhance access control and identification.

[4] Risk Management was previously labeled Target Hardening. The broader description was selected to reflect the decision-making processes inherent in determining the assets to secure, the methods and resources used to address the security, and the cost-benefit calculus associated with those decisions.

5. **Develop incentives (ordinance, legislation, or insurance ratings) to encourage CPTED at critical or mass-gathering locations and to encourage mitigation activities sponsored by public/private partnerships:**
    - Establish state laws, local ordinances and/or regulations allowing incentives for CPTED anti-terrorism initiatives;
    - Extend sovereign immunity to cover advice and consultation for CPTED construction.

6. **Assist and collaborate with the private sector to (1) identify the most serious vulnerabilities and risks, while suggesting the use of a common analytical model, (2) collaborate with the private sector to implement risk management (target hardening), and (3) inform the private sector of threats and efforts that could be taken to prevent incidents or minimize damage, in concert with the actions taken by public sector agencies;**
    - Facilitate meetings between representatives of private sector and the public sector representatives, so that they can report back to the larger private sector group, on a need to know basis;
    - Establish mutual goals and objectives by geographic region/neighborhood as well as by industry sector;
    - Analyze and document protective measures for key assets/critical infrastructure as a result of assistance provided, to maintain accountability;
    - Review legal status of mass gathering ordinances requiring certain levels of participation by private sector, and incorporate preventive measures in the requirements.

7. **Prioritize Cyber Infrastructure threats, considering vulnerability versus potential economic loss, along with target hardening plans, alert plans, and response plans.**
    - Make certain plans are consistent with the National Strategy to Secure Cyberspace (February, 2003) infrastructure protection plans;
    - Apply risk management principles to public and private infrastructure assets.

8. **As applicable and in concert with federal resources, establish perimeter and transportation security at borders and implement strict controls based on imminent threats.**

9. **Employ innovative, visible, or advertised surveillance at vulnerable or key sites, increasing the probability of recognition and capture.**
    - Use non-enforcement governmental personnel trained to use “watchout situations” to identify cues of terrorists and terrorism;

- Use law enforcement personnel to observe public and transportation movements (seat-belt checks, sobriety checkpoints, driver's license checkpoints, traffic defiles, etc.) to better observe suspicious behavior and to serve as a deterrent;
- Compile lists of commonly available devices, equipment, and materials that can be used for criminal/terrorist purposes, and train enforcement, compliance, and investigative personnel to be aware of potential value in detecting and preventing terrorist events, using "watchout situation" training.

10. **Identify and include in planning documents innovative approaches to disrupt potential actions of terrorists at strategic locations or during sensitive times.**
    - Conduct seat-belt checks, driver's license checks, or sobriety checkpoints in high risk areas;
    - Increase mobile patrols, walking patrols, mounted patrols in vulnerable areas;
    - Alter traffic patterns to disrupt ingress and egress temporarily;
    - Standardize notification procedures and reports of apartment rentals under suspicious circumstances;
    - Develop Public Service Announcements regarding health surveillance.

11. **"Vaccinate" organizations against WMD attack to make them less vulnerable by:**
    - Using mock or "red team" attacks;
    - Conducting "white level inspections" focused on prevention and risk reduction;
    - Conducting exercises using private sector assets as well as public sector resources;
    - Testing of business continuity plans through exercises and tabletops;
    - Conducting joint exercises to enhance relationships between public and private organizations.

12. **Conduct threat analysis and site surveys, to the level of training, providing assistance and recommendations to agencies, organizations and stakeholders on making assets less vulnerable.**
    - Employ CPTED experts to advise public and private organizations;
    - Balance treatment with threat, using a risk management model;
    - Publicize successes;
    - Assist private sector in recognizing the positive financial impact of WMD prevention, through tax assistance for prevention and liability protection for advanced prevention development.

13. **Conduct vaccinations, as appropriate, to reduce vulnerability to biological agents.**

14. **Establish or review quarantine authorities and include in the risk management plan and model, levels of isolation and quarantine to prevent contamination or infection of unaffected persons or places.**

15. **Consistent with a "Risk Management Model," conduct vulnerability assessments and institute procedures to secure facilities, property, equipment, and materials:**
    - Institute a culture of security-consciousness to avoid loss of uniforms or equipment that could be used to impersonate a fire, enforcement, security, or other public or safety official;
    - Ensure security accountability of key facilities, police stations, fire stations, health centers, and emergency facilities, consistent with the risk management model;
    - Include terrorism prevention security issues in building inspections and premises inspections;
    - Identify high risk and high consequence facilities, such as universities' and private laboratories' bio-storage facilities for extraordinary security awareness and accountability;
    - Monitor and secure biological and radiological samples in college and university laboratories;
    - Disperse stored resources to reduce vulnerability of sensitive materials;
    - Engage in target hardening of facilities, based on threat assessments, to include fences, access control, traffic signaling devices, and biological and radiological sensors;
    - Enhance facilities' security to reduce the threat of theft of Public Works equipment, or other similar equipment, that could be used in attacks;
    - Identify critical infrastructure, such a bridges and tunnels, for preventive observation and surveillance.

Jurisdictions seeking to improve "Threat Recognition" to halt the development of a WMD terrorism threat before it is executed should:

1. **Create a secure system to collect, screen, and store relevant information with investigative value (including Consequence Management and Medical Surveillance, Public Health data, Firefighters data, INS information, etc.) in a database, hotline, or "data warehouse," using nationally accepted definitions and protocols for "intelligence data" security and access, and that is controlled and protected at the federal level, available through a secure information portal and network, to be disseminated to those key decision-makers involved in terrorism prevention strategies and investigations, using the following processes or resources, for example:**
    - Establish a rating and criteria system to reflect the quality and urgency of information, being certain it is widely distributed and utilized to foster consistency and reliability of data, information, and intelligence;
    - Establish an intelligence database with the capacity to search existing police records management systems, identify associations among persons, organizations, locations, vehicles and incidents;
    - Establish a database, similar to secure, national databases, with information shared on a need-to-know basis among those best equipped to collect and collate that information;
    - Establish definitions consistent with established protocol, such as Foreign Affairs Manual Volume 12 (Definitions of Diplomatic Security Terms) or other accepted and established definitions;
    - Conduct intelligence operations consistent with 28 CFR 23;
    - Conduct operations consistent with American National Standard for Information Technology – Role Based Access Control;
    - Conduct operations in conjunction with the Terrorist Threat Integration Center, DHS.

2. **Train personnel to be familiar with standards for driver's licenses and other forms of identification, consistent with U.S. Identification Manual or other reference guides.**
    - Develop reference materials describing or providing information on, examples of, and criteria for:
        - driver's licenses;
        - commercial driver's licenses;
        - minor's licenses;
        - non-driver Identification cards;
        - identifying information on each form of documentation;
        - types of laminations;

- security features including bar codes and magnetic strips;
- whether license and signature are digitized for computer retrieval;
- telephone numbers for central authority for state issuance and enforcement to check validity of identification.

3. **Map threats and capabilities for preemptive action:**
    - Establish GIS and GPS capabilities, if resources permit;
    - Train personnel to access geocoded information;
    - Provide technology and equipment for immediate retrieval of geocoded information.

4. **Coordinate public safety communications to forewarn of threats:**
    - Integrate emergency warning systems for law enforcement;
    - Integrate emergency warning systems for non-law enforcement agencies;
    - Integrate public warning systems.

5. **Train law enforcement personnel and others (Fire, EMS, PW, HC, social services, etc.), using standard definitions, criteria, and terms, to recognize as clearly as possible the behavioral, observable, and legal criteria for:**
        - what constitutes suspicious activity;
        - an investigative lead;
        - a suspect;
        - an associate;
        - an inventory of behaviors and/or activities that constitute "suspicious behavior" likely to forewarn of a pending terrorism conspiracy or plot;
    - Establish protocol for identifying and responding to terrorists conducting reconnaissance/surveillance of potential targets and train personnel to recognize this behavior;
    - Train personnel on the procedures and propriety for approaching persons posing possible threats such as those taking unusual pictures/video of key sites and targets;
    - Train law enforcement to recognize commonly available, dual-use equipment and materials in context with high-risk locations;
    - Conduct random inspection of buildings, facilities, trucks/vans entering target rich environments;
    - Search or screen people and their possessions when entering large gatherings;
    - Establish extraordinary identification-verification requirements for activities linked with threats.

6. **Train law enforcement personnel to link crime analysis queries from patrol officers directly into the database with replies and cues that**

classify subjects and clearly advise as to appropriate action (i.e., update address, interview and release, photo needed, prints needed, etc.).

7. **Establish awareness of general public and the private security sector regarding the identification of terrorists surveiling potential targets and insure that the public knows what constitutes such suspicious activity, and the notification processes to advise Public Safety of the information.**

8. **Develop chemical, biological, and nuclear recognition and tracking systems in public and private sectors, consistent with threat and risk analysis models.**

9. **Locate and position detection systems and CCTV systems in key transportation, energy and infrastructure sites, consistent with a risk management model.**

10. **Establish analytical tools and linkages with non-governmental organizations to identify suspect groups via financial records, public records, and private records, with appropriate legal restrictions, shared with task forces or fusion centers.**

11. **Include in Community Policing training, the utilization of community resources in identifying suspicious activities.**

12. **Using an analytical model for risk management and vulnerability analysis, conduct threat analyses and critical site surveys to the level of training and needs, to identify those sites and facilities where threat recognition actions should be concentrated.**

13. **Develop awareness and "watchout situation" training for other than first responders (Public Works, Public Health, Health Services, social services, public utilities, school officials, etc.) using appropriate behavioral signs, equipment, materials, dual-use potential.**

14. **Establish an automatic-identification system for vessels, trucks, trains, and other transport vehicles, while maintaining security of information related to cargo that is high risk.**

15. **Enact mass gathering ordinances as protective measures, using models that have been validated, to describe equipment and personnel needs by type of gathering or event.**

16. **Consistent with an analytical risk management model, facilitate the judicious public sector response and protection of assets, and the**

sharing of information to recognize threats, based on the vulnerability and threat levels.

17. **Institute a management information system to track, locate, and monitor public sector equipment and personnel (Police, Fire, EMS, HaxMat, Military, etc.), to immediately recognize losses that could represent terrorist threats.**

18. **Maintain current and complete inventory and accountability system for hazardous materials and biological agents, even during transporting, coupled with procedures for reporting irregularities.**

19. **Ensure capability for early diagnosis of health hazards in the community, using epidemiological surveillance methods.**

20. **Train appropriate personnel to be aware of the Select Agent Program for weaponized agents.**
21. **Perform "white level" inspections, at a minimum, to discern patterns that can suggest vulnerability to terrorism, as well as safety issues.**

22. **Recognize the threat potential for land, air, water, rail, and mass transit, and other elements of the critical infrastructure, consistent with an analytical risk assessment model, and recommend appropriate prevention strategies**

Jurisdictions seeking to improve "Intervention" to stop terrorists before they can execute a threat should:

1. **Train personnel to recognize threats and threatening cues and to respond appropriately to suspects preparing for attacks.**

2. **Train law enforcement personnel in tactical capabilities with special teams of law enforcement, emergency response, and military resources, to respond quickly and appropriately in a potential terrorism event, with the objective of intervening in an impending attack.**

3. **Articulate and disseminate through general training and specific tactical training within Law Enforcement, the legal criteria for making cases, conducting wiretaps, and conducting surveillance on suspected WMD terrorists, ensuring familiarization with:**
    - Conspiracy statutes;
    - Search and seizure requirements;
    - FISA requirements;
    - Established legal criteria and procedures for intervention in suspicious circumstances and events;
    - SOPs for observing people and targets at high threat locations;
    - Laws that protect public safety information;
    - Contact lists and contact information for legal opinions and assistance.

4. **Establish pre-service and in-service training in legal, tactical, and strategic aspects of policing in the WMD terrorism environment, to enhance the ability to apprehend terrorists.**

5. **If indicated in an analytical Risk Management Model, develop plans for pre-boarding searches for mass transit vehicles in the event of a credible threat.**

6. **As indicated in an analytical Risk Management Model, establish plans and needs assessments for deployment of resources to meet known or anticipated threats to preempt or deter events.**

7. **Facilitate a prosecutorial and judicial structure, process, collaboration, and expertise that enhances successful prosecution of WMD terrorism.**

8. **Exercise the use of processes for collecting and entering investigative intelligence and retrieving information, resulting in successful intervention and arrest of terrorists.**

9. **Articulate the legal requisites for authorities to isolate and decontaminate to reduce spread of suspected diseases or agents.**

10. **Include in Risk Management plan the collateral implications to private sector in a WMD event intervention and have plans to coordinate mitigation.**

Broader WMD terrorism prevention strategies or approaches with national implications (described in National Strategy for Homeland Security):

1. Ensure that legal sanctions reflect the "certainty" of punishment for those engaging in WMD terrorism.
2. Increase perceptions of invulnerability of the Nation, sites and populations.
3. Establish presence of strategic prevention capability within national incident management system.
4. Standardize military assistance protocols for prevention.
5. Prepare, train, exercise and equip responders to engage in prevention activities and surveillance.
6. Establish coordinated standards for driver's licenses.
7. Establish a national laboratory for homeland security.
8. Release results of successful resistance to cyber attacks.
9. Develop chemical, biological, and nuclear countermeasures.

Disciplines Represented in the Abbreviations following Tasks:

Emergency Management Agency (EMA)
Emergency Medical Services (EMS)
Fire (Fire)
Governmental Administrative (GA)
Hazardous Materials (HazMat)
Public Works (PW)
Transportation (TR)
Law Enforcement (LE)
Public Health (PH)
Health Care (HC)
Public Safety Communications (PSC)
Private Sector (PS)